

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005 年 7 月 14 日 (14.07.2005)

PCT

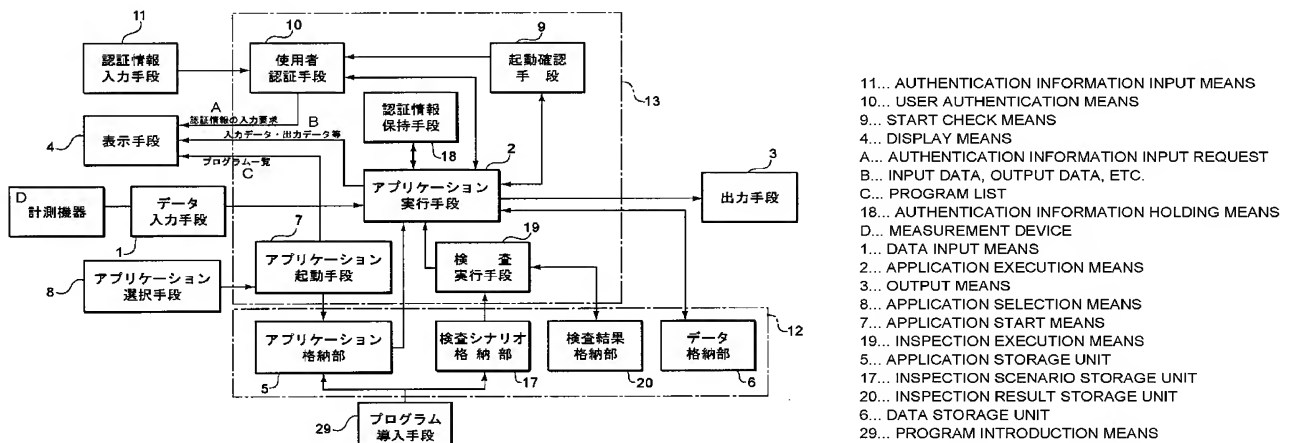
(10) 国際公開番号
WO 2005/064473 A1

- (51) 国際特許分類⁷: G06F 11/30 (71) 出願人 および
(21) 国際出願番号: PCT/JP2004/019565 (72) 発明者: 濱田 孝治 (HAMADA, Takaharu) [JP/JP]; 〒5770061 大阪府東大阪市森河内西 2-2 0-4 Osaka (JP).
(22) 国際出願日: 2004 年 12 月 27 日 (27.12.2004) (74) 代理人: 矢口 太郎, 外(YAGUCHI, Taro et al.); 〒1070062 東京都港区南青山 2-1 3-7 マトリス 4 階 大森・矢口国際特許事務所 Tokyo (JP).
(25) 国際出願の言語: 日本語 (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,
(26) 国際公開の言語: 日本語
(30) 優先権データ:
特願 2003-429897
2003 年 12 月 25 日 (25.12.2003) JP
(71) 出願人 (米国を除く全ての指定国について): 株式会社エイチ・アンド・ティー (H&T CORPORATION) [JP/JP]; 〒5770061 大阪府東大阪市森河内西 2-2 0-4 Osaka (JP).

[続葉有]

(54) Title: SAFETY TEST SUPPORT SYSTEM, METHOD, AND PROGRAM

(54) 発明の名称: 安全性試験支援システムおよび方法ならびにプログラム



(57) Abstract: [PROBLEMS] To provide a safety test support system capable of executing inspection to automatically detect a change during a system operation and surely guarantee GLP and the like. [MEANS FOR SOLVING THE PROBLEMS] The safety test support system includes: a storage unit (5) for storing applications associated with safety tests functionally divided according to a data item and/or operation; application start means (7) for starting at least one of the applications selected from the aforementioned applications; an inspection scenario storage unit (17) for storing inspection scenarios corresponding to the respective applications for detecting a change during a system operation in each application; inspection execution means (19) for successively executing the inspection scenarios of the inspection scenario storage unit (17) by input of an inspection execution signal, thereby detecting a change in each application.

(57) 要約: 【課題】システム運用中の変化を自動的に検知する検査を実行し、確実にGLP等を保証できる安全性試験支援システムを提供する。【解決手段】データ項目および/または操作ごとに機能分割された複数種類の安全性試験に関するアプリケーションを格納する格納部5と、上記複数種類のアプリケーションのうち選択された少なくともいずれかのアプリケーションを起動するアプリケーション起動手段7と、上記複数種類のアプリケーションのそれぞれに対応し、それぞれのアプリケーションにおけるシステム運用

[続葉有]



SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, YU, ZA, ZM, ZW.

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

(84) 指定国 (表示のない限り、全ての種類の広域保護
が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA,
SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ,
BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE,
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,
IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR),

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

明 細 書

安全性試験支援システムおよび方法ならびにプログラム

技術分野

- [0001] 本発明は、主として薬品を生体に投与した際の生体の体重・接餌量・摂水量・生化学検査・臨床症状観察・病理所見・尿量・眼科学的検査・血液学的検査等を記録・管理・集計する薬品試験データ管理等に適用可能で、特に、生体として動物を用いた薬品の毒性試験に好適な安全性試験支援システムおよび方法ならびにプログラムに関するものである。

背景技術

- [0002] 医薬品・農薬・食品添加物・その他化学物質の発癌性や毒性等、人体に対する安全性は、市販に先立って臨床試験が行われるが、臨床試験に入る前に、ラットやマウス等の動物を使用する非臨床試験で確認することが行われている。
- [0003] このような動物を使用した薬品等の安全性試験には、：1回あたりどの程度投与すれば毒性が発生し、その毒性の特徴が何かを明らかにする単回投与毒性試験；反復投与毒性試験；親動物の生殖に及ぼす影響や次世代の発生に関する影響等を明らかにする生殖・発生毒性試験；DNAに障害性を示す物質や突然変異を誘発する性質の有無を明らかにする変異原性試験；癌原性試験；皮膚感作性試験、皮膚光感作性試験；依存性試験；がある。
- [0004] 上記各試験は、薬品を実際に動物に投与し、体重、餌、水、尿等の量の測定や臨床症状の観察・病理組織所見等を行い、採取したデータを集計し、分析することによって行われる。
- [0005] このような安全性試験は、その薬品を実際に人体に投与して行う臨床試験に先立って行われる。そして、最終的に人体に影響を及ぼす影響を調べるために、薬品が生体に及ぼす影響を正確に理解し、分析することが必要になる。このため、データの記録や管理・分析には、従来からコンピュータシステムが利用されてきた（例えば下記の特許文献1）。また、医薬品をはじめとする薬品は人体に影響を与えるものであるため、上記のような安全性試験のデータ管理には、データに改ざんが加えられること

のないよう、厚生省をはじめとする各官庁で厳しい基準が設けられている。このような基準は、総称して「GLP (Good Laboratory Practice)」と呼ばれ、当然のことながら、データを管理するコンピュータシステムは、GLPの基準を満たしている必要がある。

[0006] すなわち、まず、システムを導入した際に、GLPに適合して確実に動作するか否かを確認する導入時の動作確認(バリデーション)が必要である。また、システムの運用が開始されてからも、システムの一部に考慮しなければならない変更があったような場合には、GLPに適合して確実に動作することをシステム全体について再度確認(バリデーション)して文章として残し、データやシステムに改ざんがないことを保証していかなければならない。

[0007] このようなシステムの導入及び運用は、市場は非常にニッチで独特のノウハウが必要なため、非常に高額となる。

[0008] 特許文献1:特開平7-110325号
特許文献2:特開平10-275093号

発明の開示

発明が解決しようとする課題

[0009] ところで、従来の安全性試験のシステムは、それが異なる複数の機能からなる場合であっても、1つのシステムとして導入・運用され、システム全体としてGLPを保証するようになっている。このため、システムの一部のアプリケーションプログラムにバージョンアップ等があった場合でも、再度システム全体として動作確認を行わなければならないということがあった。

[0010] 例えば、近年はシステムのセキュリティーホールを悪用したウィルスプログラムのようなシステム破壊プログラムが蔓延しているため、オペレーションシステム(OS)の供給メーカによる頻繁なセキュリティパッチの提供が行われている。そして、システムを安全に運用するためには、セキュリティパッチの提供があったときには迅速にアップデートを行うことが不可欠になっている。

[0011] しかしながら、従来のように全体としてGLP等を保証するようなシステムでは、オペレーションシステムにセキュリティパッチを当てるだけでもシステム全体として変更され

たことになるため、バリデーションを行う必要が生じる。このような運用途中での動作確認は、通常2〜3名の人員で3ヶ月以上の時間を要する。このため、システム導入時の受入検査は一通り行われるものの、一旦システム稼動をはじめると、運用開始後の機能アップ等に起因する動作確認等は、実質的には全く行えなかったのが実情である。したがって、現実的な運用方法としては、動作確認を行わないで済むように、アップデートや機能アップを全く行わないまま運用を続けるしかなかったのである。

[0012] このような事情から、運用開始後にセキュリティホールが発見されたような場合でも、セキュリティパッチを当てることもできず、システムの安全性が危惧される状態のままでの運用が続けられている。また、ソフトウェア自体は汎用のハードウェアで利用できるものの、汎用機として運用するとオペレーションシステムや連携していない他のソフトウェアのアップデートだけでも動作確認が必要になってしまうため、実質的には専用機を準備して運用しなければならず、システムの導入コストも非常に高いものとなっていた。

[0013] また、システムの動作確認を行うシステムは、各種のものが開示されている（例えば上記特許文献2）。しかしながら、従来の動作確認システムは、主として「開発中」のプログラムのバグを見つけて修正するために使用されるものであるため、動作確認の結果に少しでも変化があると、それを検知してNG出力するようになっている。ところが、このような動作確認システムを「運用中」の安全性試験支援システムに適用しようとすると、例えば、フォントが少し変わったとか、表示の色彩が少し変わったというような、GLP等を保証して安全性試験支援システムを運用する上で全く影響しないレベルの変化であっても「バグ」や「変化」として検知し、NG出力してしまうため、それらのNG出力をすべて人間の目で再確認する必要があった。したがって、自動検査であったとしても、現実には検査や動作確認に相当のマンパワーを要することになっていた。

[0014] しかも、従来のように全ての機能が一体化されたシステムでは、ほとんど使用されることのない機能が数多く付加されており、このような無駄な機能が付加されることによってもシステムの起動時に使用者の認証を行うものの、その後は途中で入力者等に変更があってもシステムを終了させるまでそのまま稼動されるため、実質的に入力者の確定ができておらず、GLP等を保証する上で問題があった。

- [0015] 本発明は、このような事情に鑑みなされたもので、システム運用に影響する変化を自動的に検知でき、かつ、確実にGLP等の基準を満たしていることを保証することができるコンピュータソフトウェアプログラムを提供することを目的とする。

課題を解決するための手段

- [0016] この発明の第1の観点によれば、互いに関連しコンピュータシステム上で実行される1もしくはそれ以上のアプリケーションプログラムのいずれか1つもしくはそれ以上に所定の変更がなされたか否かを検出するためのコンピュータソフトウェアプログラムであって：記憶媒体と；前記記憶媒体に格納され、前記アプリケーションプログラムのうち少なくとも最初の1つを実行する前にユーザの認証を行い、以後実行されるアプリケーションプログラムに前記認証にかかるユーザを関連付ける認証プログラムと；前記記憶媒体に格納され、各アプリケーションプログラムに関連付けられ、各アプリケーションプログラムに所定の変更がなされたかを検出するための検査シナリオと；前記記憶媒体に格納され、検査プログラムが関連付けられた所定のアプリケーションプログラムを前記検査シナリオに従って実行させることにより、そのアプリケーションプログラムに所定の変更がなされたかを検知させ、その検知結果を前記ユーザ名及びアプリケーションプログラムと関連付けて出力させる検査プログラムと；を有することを特徴とするコンピュータソフトウェアプログラムが提供される。ここで、このコンピュータソフトウェアプログラムは、例えば、安全性試験の結果が前記アプリケーションプログラム中で改ざんされていないことを保証（バリデーション）するためのものであり、前記アプリケーションプログラムは、安全性試験用の計測デバイスから改ざんされていない計測値を受け取りこの測定値を処理して所定の処理結果を出力するものである。
- [0017] すなわち、本発明は、例えば、データ項目および／または操作ごとに機能分割された関連する複数のアプリケーションプログラムから構成された安全性試験用のシステムに適用されることが最も好ましい。この発明によれば、一部のアプリケーションプログラムに何らかの変更がなされた場合に、すでに一度行われたバリデーションに基づいて許容できる以上の変更がなされたか否かについてアプリケーションプログラム毎に検知し、その結果を示したユーザに関連付けて出力・記録することができる。このことにより、バリデーションが有効かについて確実に保障することができる。

- [0018] 本発明の1の実施形態によれば、前記1もしくはそれ以上のアプリケーションプログラムは、他のアプリケーションプログラムをユーザに選択実行可能に表示するアプリケーションプログラムランチャーを含むものである。
- [0019] このような構成によれば、ユーザが、本発明の対象として互いに関連付けられた複数のアプリケーションソフトウェアプログラムを容易に認識し、管理することができる。
- [0020] 本発明の別の1の実施形態によれば、前記1もしくはそれ以上のアプリケーションプログラムは、同一ポリシーの下で所定の基準を満たすために動作確認が必要な複数のアプリケーションプログラムを有し、前記検査シナリオは、各アプリケーションプログラムになされた変更が、このアプリケーションプログラムを再度の動作確認を行うことなく実行することを許容する程度のものか否かを検出するためのものであり、前記検査プログラムは、そのアプリケーションプログラムに、前記検出シナリオに従って、動作確認を行うことなく実行することを許容する程度以上の変更がなされたかと検出したときに、前記そのことを表示するように前記コンピュータシステムに指令するものである。ここで、前記ポリシーには、「GLP (Good Laboratory Practice)」等の安全性データの管理に関するポリシーが含まれる。
- [0021] また、更なる別の1の実施形態によれば、前記検査プログラムは、前記検査シナリオに従って、前記アプリケーションプログラムに擬似信号を入力し、上記入力した擬似信号に対する応答信号を検査することにより、アプリケーションプログラムに所定の変更がなされたかを検知させるものである。この検査シナリオは、検査するアプリケーションプログラムを特定するための情報と、そのアプリケーションプログラムに擬似信号として入力する情報と、そのデータに対する応答に関する許容範囲に関する情報を少なくとも含むものであることが好ましい。
- [0022] このような構成によれば、アプリケーション毎に精度の高いシナリオを用意しておき、アプリケーションにこのシナリオに基づいた処理を行わせ、その応答信号に基づいて所定の変更を検出することができる。なお、ここで擬似信号とは、検査シナリオに基づいて検査プログラム若しくはその他のプログラム(OSのイベントプログラム等)で生成される信号であり、ユーザがキーボード等から入力するものではない。
- [0023] 更なる別の1の実施形態によれば、前記検査プログラムは、所定の周期で起動され

るものである。

- [0024] 更なる別の1の実施形態によれば、前記検査プログラムは、前記検知結果をコンピュータディスプレイ上に表示させる検知結果表示部と、当該検知結果に対するユーザの入力を受け取って前記検知結果と関連付けて出力するユーザ入力出力部とを有する。
- [0025] 更なる別の1の実施形態によれば、前記認証プログラムは、所定時間毎にユーザに認証情報の入力を求める認証更新要求部を有し、前記認証更新要求部でユーザの認証ができない場合には、当該ユーザに関連付けられた実行中の前記アプリケーションプログラムを終了させるようになっている。
- [0026] 更なる別の1の実施形態によれば、前記認証プログラムは、最初のユーザ認証の後に、ユーザの要求に応じて再度ユーザ認証を行い、現在実行されているアプリケーションプログラム及び以後実行されるアプリケーションプログラムに前記認証にかかるユーザに関連付けるものである。
- [0027] 本発明の第2の主要な観点によれば、互いに関連する1もしくはそれ以上のアプリケーションプログラムを格納するアプリケーション格納部と、前記アプリケーションプログラムのうち少なくとも最初の1つを実行する前にユーザの認証を行い、以後実行されるアプリケーションプログラムに前記認証にかかるユーザに関連付ける認証部と、各アプリケーションプログラムに関連付けられ、各アプリケーションプログラムに所定の変更がなされたかを検出するための検査シナリオを格納する検査シナリオ格納部と、検査プログラムが関連付けられた所定のアプリケーションプログラムを前記検査シナリオに従って実行させることにより、そのアプリケーションプログラムに所定の変更がなされたかを検知させ、その検知結果を前記ユーザ名及びアプリケーションプログラムと関連付けて出力させる検査部と、を有することを特徴とするアプリケーションプログラム検査システムが提供される。
- [0028] 本発明の第3の主要な観点によれば、互いに関連し、コンピュータシステム上で実行される1もしくはそれ以上のアプリケーションプログラムのいずれか1つもしくはそれ以上に所定の変更がなされたか否かを検出するための方法であって、前記アプリケーションプログラムのうち少なくとも最初の1つを実行する前にユーザの認証を行い、

以後実行されるアプリケーションプログラムに前記認証にかかるユーザを関連付ける認証工程と、各アプリケーションプログラムに関連付けられ各アプリケーションプログラムに所定の変更がなされたかを検出するための検査シナリオを用い、検査プログラムが関連付けられた所定のアプリケーションプログラムを前記検査シナリオに従って実行させることにより、そのアプリケーションプログラムに所定の変更がなされたかを検知させ、その検知結果を前記ユーザ名及びアプリケーションプログラムと関連付けて出力させる検査工程と、を有することを特徴とする方法が提供される。

- [0029] 本発明においては、上記検査プログラムは、検査されたシステム運用中の変化のうち、システムの運用に影響しない変化を検知した場合には変化とみなさず、システムの運用に影響する変化を検知した場合には変化として検知する場合には、従来のシステムのように全ての変化を「変化」としてNG出力するのではなく、例えば、フォントが少しかわったとか、表示の色彩が少しかわったというような、GLP等を保証して安全性試験支援システムを運用する上で全く影響しないレベルの変化は「変化」とみなさないことにより、人間の目によるNG出力の再確認を大幅に減少させることができる。
- [0030] また、本発明においては、上記検査実行手段による各アプリケーションプログラムの検査は、検査プログラムが検査対象とするアプリケーションプログラムを特定し、当該特定されたアプリケーションプログラムに対して直接に擬似信号を入力し、上記入力した擬似信号に対する応答信号を検知し、検知した応答信号を検査開始前のものと比較することにより行なわれる場合には、アプリケーションプログラムに対して直接に擬似信号を入力することから、デバイスやドライバの要因が排除された純粋なシステムの変化を検知することができる。したがって、デバイスやドライバを変更したような場合でも、運用や検査に影響を与えないため、システムの使いやすさが確保される。
- [0031] 本発明においては、上記擬似信号の入力は、オペレーションシステムを経由せずに行なう場合には、オペレーションシステムを経由せずにアプリケーションプログラムに対して直接に擬似信号を入力することから、デバイスやドライバだけでなく、オペレーションシステムの要因もが排除された純粋なシステムの変化を検知することができる。
- [0032] 本発明において、上記擬似信号の入力は、オペレーションシステムを経由して行な

う場合には、オペレーションにシステムを経由してアプリケーションプログラムに対して直接に擬似信号を入力することから、オペレーションにシステムを含めたシステムの変化を検知することができる。

[0033] 本発明において、上記プログラム格納部に格納されたアプリケーションプログラムの一覧を表示する表示手段と、上記表示手段に表示されたアプリケーションプログラムの一覧から起動を望むアプリケーションプログラムを選択するプログラム選択手段と、上記プログラム選択手段で選択されたアプリケーションプログラムを起動する起動手段と、上記起動されたアプリケーションプログラムのうちいずれかが起動しているか否かを所定時間ごとに確認する起動確認手段と、上記起動確認手段によりいずれかのアプリケーションプログラムの起動が確認され続けている間、所定期間ごとに使用者の認証情報の入力を求める使用者確認手段とを備えている場合には、システムの起動時に使用者の認証を行い、その後に途中で入力者等に変更があったとしても、起動されたアプリケーションプログラムのいずれかが起動し続けている間、所定期間ごとに使用者の認証を行なうため、実質的に入力者が確定でき、確実にGLP等を保証することができる。

[0034] 本発明において、使用者確認手段による使用者確認の有効性情報を保持する認証情報保持手段を備え、各アプリケーションプログラムの起動の際に、上記認証情報保持手段に保持された有効性情報に基づいて、認証が有効な場合にアプリケーションプログラムの実行を開始し、認証が無効な場合にアプリケーションプログラムの実行を開始しないようになっている場合には、使用者認証が有効であればアプリケーションプログラム起動ごとの使用者認証を行わないため、重複する手間が省けて使い勝手がよい。

[0035] 本発明において、登録されたアプリケーションプログラムが起動されたときに上記アプリケーションプログラムが使用者認証手段の起動を確認し、使用者認証手段が起動されていない場合に使用者認証手段を起動させるようになっている場合には、ひとつの使用者認証手段で複数のアプリケーションプログラムの認証を管理できるため、いずれかのアプリケーションプログラムが起動されている間、他のアプリケーションプログラムを起動するたびに使用者の認証を行なう必要がなくなるため、作業効率が向

上する。また、登録されたアプリケーションプログラム以外のアプリケーションプログラムの実行中に使用者認証手段が起動されないため、必要以上にメモリ容量を消費せず、そのために実行速度が低下する等の弊害が生じない。

- [0036] 本発明において、生体として動物を用いた薬品の毒性試験に用いられるものである場合には、生体として動物を用いた薬品の毒性試験が、膨大で多種多様なデータが存在し、ユーザによって必要なデータの種類の異なることが多いため、使用する可能性の高い必要なアプリケーションプログラムだけ導入でき、システム全体のコストを大幅に引き下げることができる。また、複数の観察者が交代でデータ入力等を行なうこともありうるため、一定期間ごとに入力者等が確認できる本発明の効果が顕著であり効果的である。

発明を実施するための最良の形態

- [0037] つぎに、本発明を実施するための最良の形態を説明する。

- [0038] 図1は、本発明の安全性試験支援システムの一実施の形態を示すシステム構成図である。このシステムは、本発明を薬品試験データ管理システムに適用した例を示すものであり、薬品を実際に動物に投与した時の体重、餌、水、尿等の量や生化学検査、血液学的検査、臨床症状の観察、各種の病理所見等のデータを入力するデータ入力手段1と、このデータ入力手段1に入力されたデータを受信して、後述する各アプリケーションプログラム(以下「アプリケーション」という)を実行してデータの集計等を行なうアプリケーション実行手段2とを備えている。

- [0039] ここで、データ入力手段1は、キーボードやマウスの他、例えば、電子天秤、電子顕微鏡、濃度計等の計測機器であり、これらの機器の測定値が前記アプリケーションに直接渡されるようになっていることが好ましい。

- [0040] また、上記システムには、上記アプリケーション実行手段2で集計等されたデータ等を帳票等に出力するプリンタ等の出力手段3と、データ入力時やデータ出力時等に各種の情報を表示するディスプレイ等の表示手段4とが設けられている。さらに、入力されたデータをアプリケーション実行手段2を経由して格納するデータ格納部6とを備えている。図において、12はハードディスクやMO等の記憶装置であり、13はCPUおよびメモリ等を備えた演算部である。

- [0041] ここで、上記システムは、上述した各手段により、通常のデータ入力や集計等の処理が行なわれるようになっている。すなわち、データ入力手段1で入力されたデータは、アプリケーション実行手段2を介してデータ格納部6に格納され、入力作業中には、入力されたデータの他、必要な情報が表示手段4に表示されるようになっている。また、入力されたデータの集計や処理等を行なった場合には、集計や処理データが出力手段3から出力され、出力されるデータの他必要な情報が表示手段4に表示されるようになっている。
- [0042] そして、上記システムには、複数の業務用のアプリケーションを格納する本発明の第1プログラム格納部として機能するアプリケーション格納部5を備えている。上記アプリケーション格納部5には、例えば、体重の入力・体重の集計・体重の集計データの出力・病理所見の入力・病理所見の集計・病理所見の出力等、データ項目および／または操作ごとに機能分割された複数のアプリケーションが格納されている。上記アプリケーション格納部5に格納されるアプリケーションは、CD-ROM等の記憶媒体に格納された状態で搬送され、CD-ROMドライブ等のプログラム導入手段29を介してコンピュータのハードディスクにインストールすることにより随時導入しうようになっている。
- [0043] また、上記システムには、上記アプリケーション格納部5に格納された各アプリケーションが登録され、上記登録されたアプリケーションのうち使用者によって選択されたアプリケーションを起動するアプリケーション起動手段7(ランチャープログラム)を備えている。また、アプリケーション格納部5には、各アプリケーション格納場所とアプリケーション起動手段7へのプログラムの登録場所とが関連付けられた状態で格納されている。この関連付けは前記アプリケーション起動手段7(ランチャープログラム)に登録される。
- [0044] さらに、上記アプリケーション起動手段7に登録されたアプリケーションの一覧は、表示手段4に表示されるようになっており、上記表示手段4に表示されたアプリケーションの一覧から使用者が起動を望むアプリケーションを選択するアプリケーション選択手段8を備えている。なお、前記アプリケーション起動手段7を、前記アプリケーションの一つと捕らえて、プログラムとして前記アプリケーション格納部5に格納しておいて

も良い。

- [0045] 上記アプリケーション選択手段8によるアプリケーションの選択には、例えば、マウス等の入力用のデバイスが用いられ、図2に示すように、表示手段4の画面16上に表示されたメニュー14に表示されたアプリケーション一覧のなかから、起動を希望する所望のプログラムを選び、そのアイコン15にマウスのポインタ(図示せず)を合わせてクリックすることにより行なわれる。なお、アプリケーションはひとつだけ起動させてもよいし、ふたつ以上を起動して同時に実行させることもできる。
- [0046] そして、アプリケーション選択手段8で選択されたアプリケーションは、上述した関連付け情報に基づいてアプリケーション起動手段7によって起動される。アプリケーションの起動はアプリケーション格納部5からアプリケーションをメモリ内に読み出して展開し、オペレーションシステムから実行権限を取得することにより行なわれる。そして、起動されたアプリケーションは、アプリケーション実行手段2により実行されるようになっている。
- [0047] さらに、上記システムには、アプリケーション起動手段7で起動され、アプリケーション実行手段2で実行されているアプリケーションが、起動されつづけているか否かを所定時間(例えば5分)ごとに確認する起動確認手段9が設けられている。この起動確認動作は、アプリケーションがメモリ上に展開され実行されているかどうかをオペレーションシステムに問合せることにより行なわれる。
- [0048] また、上記起動確認手段9によりいずれかのアプリケーション起動が確認され続けている間、所定期間(例えば30分)ごとに使用者の認証情報の入力を求める使用者認証手段10が設けられている。さらに、上記使用者認証手段10の認証情報入力の要求に応じ、認証情報を入力する認証情報入力手段11が設けられている。ここで、認証情報の入力を要求する期間(認証時間)は、アプリケーションの起動を確認する時間(起動確認時間)よりも長くなるよう設定されている。
- [0049] 上記情報入力の要求は、例えば、表示手段4にパスワードの入力を促すパスワード入力画面を表示することにより行なわれる。また、認証情報の入力には、例えばキーボード等のデバイスが用いられ、前記認証情報入力手段11を利用して上記パスワード入力画面にパスワードを入力することにより行なうことができる。

- [0050] さらに、上記起動確認手段9は、アプリケーション起動手段7に登録されたアプリケーションが起動されたときに上記アプリケーションが認証プログラム(使用者認証手段10)の起動を確認し、起動確認手段9が起動されていないならば、上記アプリケーションによって起動されるようにしてもよい。このようにすることにより、ひとつの使用者認証手段10で複数のアプリケーションの認証を管理できるため、いずれかのアプリケーションが起動されている間、他のアプリケーションを起動するたびにパスワード入力等の使用者の認証を行なう必要がなくなるため、作業効率が向上する。また、登録されたアプリケーション以外のアプリケーションの実行中に起動確認手段9が起動されないため、必要以上にメモリ容量を消費せず、実行速度が低下する等の弊害が生じない。なお、本発明の認証プログラムは、前記認証情報入力手段11、使用者認証手段10および起動確認手段9によって構成される。
- [0051] また、このシステムは、アプリケーション実行手段2で実行される業務用のアプリケーションが、認証プログラム(使用者認証手段10)を起動するようになっている。また、このシステムは、使用者認証手段10による認証の有効／無効にかかる認証情報を保持する認証情報保持手段18を有し、業務用のアプリケーションが認証プログラムと交信して業務プログラム自体の実行を継続するか否かを判断するようになっている。さらに、認証プログラムは、それ自体が何度も起動してしまわないように、それ自体が終了を判断するようになっている。
- [0052] さらに、上記システムは、上記複数種類のアプリケーションのそれぞれに対応し、それぞれのアプリケーションにおけるシステム運用中の変化を検知するための複数種類の検査シナリオを格納する本発明の第2プログラム格納部として機能する検査シナリオ格納部17を備えている。また、マウスやキーボード等の入力用デバイスからの検査実行信号の入力により、上記検査シナリオ格納部17の検査シナリオを順次実行することにより、各アプリケーションにおける変化を検知する検査実行手段19を備えている。
- [0053] ここで、図3に示すように、業務アプリケーション27と検査シナリオ28がそれぞれ複数種類ずつ、すなわち、1つの業務アプリケーション27に対して1つの検査シナリオ28が対応するよう準備されている。図示した例では、アプリケーションA、アプリケーシ

ョンB、アプリケーションCに対して、それぞれ検査プログラムa、検査シナリオb、検査シナリオc、が対応している。

- [0054] これらの業務アプリケーション27および検査シナリオ28は、いずれも上記プログラム導入手段29から適宜導入することができる。すなわち、運用を開始してから業務アプリケーション27を補充的に導入するような場合、補充する業務アプリケーション27だけでなく、それに対応した検査シナリオ28も同時に導入される。このように、常に、業務アプリケーション27と検査シナリオ28とは1対1のセットで導入され使用される。
- [0055] ここで、検査シナリオは、検査するアプリケーションプログラムを特定するための情報と、そのアプリケーションプログラムに擬似信号として入力するための情報と、そのデータに対する応答に関する許容範囲(許容値)に関する情報を少なくとも含むものである。
- [0056] このように、データ項目および／または操作ごとに機能分割された複数の業務アプリケーション27が独立して存在するため、一部のアプリケーション27にバージョンアップ等があった場合でも、システム全体の検査を行なうのではなく、そのアプリケーション27に対応する検査シナリオ28だけを実行して検査を行なうこともでき、システム運用開始後の検査や動作確認の手間を大幅に削減し、検査を確実に行なうことができるようになる。また、各業務アプリケーション27に対応する検査シナリオ28を順次周期的・自動的に実行することにより、システム全体の検査や動作確認を自動的に行なえることから、システム全体の検査や動作確認も迅速かつ容易に行なうことができる。したがって、例えばオペレーションシステムにセキュリティパッチを当てるようなアップデートを行なうたびに、システムの自動検査を確実に行なうことができるようになる。
- [0057] また、システム全体の検査や動作確認を迅速かつ容易に行なえることから、セキュリティパッチ等の供給があったときには迅速にアップデートしたうえで検査を行ない、安全性の高い状態での運用が可能になる。このように、システムのバージョンアップやアップデートのたびに容易に検査や動作確認を行い、バージョンアップやアップデートにともなう運用中の変化があった場合にはそれを検知することにより、確実にGLP等を保証することができるようになる。さらに、データ項目および／または操作ごとに機能分割された複数のアプリケーション27が独立して存在するため、使用する可能

性の低い不要なアプリケーション27は導入しなくてもすむため、システムの導入コストや運用コストを大幅に引き下げることができる。

[0058] また、図3に示すように、上記検査実行手段19(検査プログラム)による各アプリケーション27の検査は、検査シナリオ28により検査対象とするアプリケーション27を特定し、当該特定されたアプリケーション27に対して直接に擬似信号を入力し、上記入力した擬似信号に対する応答信号を検知し、検知した応答信号を検査開始前のものと対比することにより行われる。

[0059] すなわち、通常の操作信号は、マウスやキーボード等の入力用のデバイス21によって入力され、このデバイス21で発生した物理信号が、当該デバイス21用のドライバ22により意味の在る操作信号に変換され、オペレーションシステム23を介して各アプリケーション27に対して入力される。本発明の検査シナリオ28によれば、通常、デバイス21から入力されてドライバで変換された操作信号と同様の擬似信号を発生させ、オペレーションシステム23を介さずに、あるいはオペレーションシステムを介して、直接的にアプリケーション27に対して入力するのである。そして、この検査実行手段19は、上記擬似信号の入力に対してアプリケーション27が応答した応答信号を検知し、この検知した応答信号を検査結果格納部20に格納された検査開始前の応答信号と対比し、検査シナリオ28に記述されている許容範囲以上であれば、変化があったとしてNG信号を出力し、そうでなければ無視して検査を続行することが行なわれるのである。なお、NG信号は、変化が検出されたことを表示する画面をディスプレイ上に表示することによって行われ、この表示はユーザが確認するまで表示される。検査実行手段19は、ユーザが確認した場合、前記変化の事実と、これを確認したユーザ名(使用者認証手段10から取得)とを関連付けて、ログとして出力・記録する。

[0060] このように、アプリケーション27に対して直接に擬似信号を入力することから、デバイス21やドライバ22の要因が排除された純粋なシステムの変化を検知することができる。したがって、デバイス21やドライバ22を変更したような場合でも、運用や検査に影響を与えないため、システムの使いやすさが確保される。

[0061] ここで、上記擬似信号の入力は、オペレーションシステム23を経由せずに行なうようにすることができる。このようにすることにより、オペレーションシステム23を経由せず

にアプリケーション27に対して直接に擬似信号を入力することから、デバイス21やドライバ22だけでなく、オペレーションシステム23の要因もが排除された純粋なシステムの変化を検知することができる。

[0062] また、上記擬似信号の入力は、オペレーションシステム23を経由して行なうようにすることもできる。このようにすることにより、オペレーションシステム23を経由してアプリケーション27に対して直接に擬似信号を入力することから、オペレーションシステム23を含めたシステムの変化を検知することができる。したがって、オペレーションシステム23にセキュリティパッチを当てたようなアップデートを行なった場合でも、それを加味したシステムの変化を検知することができ、GLPを確実に保証することができる。このように、オペレーションシステム23のアップデートを頻繁に行なったうえで検査を行ない、安全性の高い状態での運用が可能になる。

[0063] このとき、上記検査シナリオ28は、検知されたシステム運用中の変化のうち、システムの運用に影響しない変化を検知した場合には変化とみなさず、システムの運用に影響する変化を検知した場合に変化として検知するように構成されている。

[0064] すなわち、擬似信号の入力に対してアプリケーション27が応答した応答信号について、変化の有無(OKかNGか)を判定する際に、当該応答信号が以前のシステム状態から変化なしとしてOKと判定する所定の基準範囲を設定しておき、応答信号が当該基準範囲内であれば変化なし(OK)とし、上記基準範囲を超えた場合に変化として検知する(NG)ようになっている。

[0065] 例えば、擬似信号の入力に対する応答信号に多少の変化があった場合でも、当該変化がフォントの大きさが少し変わったとか、表示の色彩に多少の変化があったようなものは、システムの運用上全く問題がないレベルの変化である。このような変化をすべてNGとしていると、NG出力の頻度が膨大になり、それぞれのNG出力に対して結局人間が目視と手動操作で処理を行わなければならなくなる。そこで、従来のシステムのようにすべての変化を「変化」としてNG出力するのではなく、上記のような基準範囲を設定し、例えば、フォントが少し変わったとか、表示の色彩が少し変わったというような上記基準範囲内のGLP等を保証して安全性試験支援システムを運用する上で全く影響しないレベルの変化は「変化」とみなさないことにより、人間の目による

NG出力の再確認を大幅に減少させることができる。

- [0066] 図4は、上記システムの動作を示すフローチャートである。なお、図において「S」は、ステップを意味する。
- [0067] まず、システムの導入時に、受入検査が開始される。この受入検査では、体重、餌、水、尿等の量や病理所見等のデータがデータ入力手段1(すなわち電子天秤等の各種デバイス21)によって入力され、アプリケーション実行手段2に集計等を行なわせて正確な集計結果が得られることを確認する。また、検査実行手段19によって検査シナリオ28を実行し、当該検査シナリオ28が正常動作するか否かの確認が行なわれる。
- [0068] このとき、検査結果格納部20には、上記受入検査における体重、餌、水等のデータ入力と、入力されたデータの集計等の処理や動作結果が記憶される。このとき、上記各動作結果について、前記シナリオ28における所定の基準範囲が設定されることが好ましい。ただし、これに限定されるものではなく、前記基準範囲を測定結果によらずに決定しても良い。
- [0069] 受入検査が終了すると、システムの実際の運用が開始される。そして、通常の業務内では、動作確認を実行せずにシステムの運用が続けられる。
- [0070] そして、通常の運用においては、つぎのようにして動作する。
- [0071] すなわち、まず、ランチャープログラム(アプリケーション起動手段7)を起動することにより、登録されているプログラムの一覧が表示手段4に表示される(S10:図2参照)。ついで、表示手段4の画面16に表示されたメニュー14のなかから、所望するプログラムのアイコン15をクリックして所望の業務プログラムが選択されると(S20)、業務用アプリケーションの起動が開始される(S30)。そして、起動させたアプリケーションを実行して、体重、餌、水、尿等の量や病理症状の観察所見等のデータ入力や、入力データの集計、集計データの帳票出力等の各アプリケーションに応じた処理が行なわれる。そして、ランチャープログラムを終了しない場合はステップ10に戻り、そうでない場合は終了する(S40)。
- [0072] ステップ30において業務用アプリケーションの起動が開始されると、認証プログラム(起動確認手段9)の起動が開始される(S50)。認証プログラムが起動されると、ステ

ップ90に進み、認証プログラムが既に実行されているか否かの確認がおこなわれ、既に実行されていれば2重起動を防止するために認証プログラムの起動動作は終了し、実行されていなければステップ100に進む。

[0073] ステップ100では、認証情報入力手段11に対してパスワードやユーザID等の認証情報の入力を要求する。ステップ110では、ステップ100において入力されたパスワードやユーザIDが正当で有効であるか無効であるかを判断する。ステップ110において、認証が有効であれば、業務用アプリケーションに認証有効の通知を行い、認証情報保持手段18に認証有効の情報を保持する(S115)。一方、ステップ110において、正確なパスワードが入力されず、認証が無効であれば、業務用アプリケーションに認証無効の通知を行い、認証情報保持手段18に認証無効の情報を保持する(S120)。

[0074] ここで、ステップ110において、入力されたパスワードが誤っている等、正確な認証情報が入力されなければ再び認証情報の入力を要求し、一定回数繰り返しても正確なパスワードが入力されず、使用者の認証ができなかった場合は、一時停止状態であるアプリケーションに対して実行の強制終了を指示し、アプリケーションは終了指示を受けて終了するようにしてもよい。

[0075] ついで、使用者の認証を行う認証時間(例えば30分、ただし有効な範囲でユーザが自由に設定できることが好ましい)の経過を待つ(S130)。ステップ130において上記認証時間が経過していればステップ100に戻り、再度認証情報の入力を要求する。ステップ130で上記認証時間が経過していなければ、業務用アプリケーションの実行確認時間が経過しているか否かを判定する(S140)。ステップ140において、上記実行確認時間が経過していなければステップ130に戻り、再度認証時間の経過を待つ上述した動作を繰り返す。ステップ140において上記実行確認時間が経過していれば業務用アプリケーションが実行されているか否かの確認を行なう(S150)。そして、ステップ160において業務用アプリケーションが1つでも実行されていればステップ130に戻り、再度認証時間の経過を待つ上述した動作を繰り返す。ステップ160においてアプリケーションプログラムが1つも実行されていなければ、認証プログラムを終了する。

- [0076] 一方、ステップ30においてアプリケーションの起動が開始され、ステップ50において認証プログラムの起動が開始されたのち、ステップ60に進み、上記認証プログラムとの通信により認証情報保持手段18に保持された認証の有効／無効に係る情報の確認を行なう。
- [0077] ステップ70において、認証情報保持手段18に保持された認証が有効であれば、ステップ80に進み、業務用アプリケーションが実行され、無効であれば業務プログラムの起動処理が終了する。なお、認証が有効な場合、前記アプリケーションに認証にかかるユーザ名が記録され、アプリケーションと現在ログインしているユーザとが関連付けられる。なお、この関連付けは、アプリケーションとユーザ名を直接関連付ける場合に限らず、アプリケーションの起動及び終了時間のログとユーザのログインとログアウトの時間のログとを後から突合可能に記録する方法によっても良い。
- [0078] このように、上記システムによれば、起動されたアプリケーションのいずれかが起動しつづけている間、所定期間ごとに使用者の認証を行うため、実質的に検査結果の確認者が確定でき、確実にGLP等を保証することができる。また、データ項目および／または操作ごとに機能分割された複数のプログラムが独立して存在するため、一部のプログラムにバージョンアップ等があった場合、そのプログラムだけの動作確認を行えばすむようになる。したがって、システム運用開始後の動作確認を確実に行ってGLP等を保証することができるようになる。また、使用する可能性の低い不要なプログラムは導入しなくてもすむため、システム全体のコストを大幅に引き下げることができる。
- [0079] また、認証プログラムが一旦ユーザ認証を行っていれば、業務プログラムを起動するごとのユーザ認証を行わないため、重複する手間が省け、使い勝手がよい。
- [0080] また、ひとつの使用者認証手段で複数のアプリケーションの認証を管理できるため、いずれかのプログラムが起動されている間、他のアプリケーションを起動するたびに使用者の認証を行う必要がなくなるため、作業効率が向上する。また、登録されたアプリケーション以外のアプリケーションの実行中に使用者認証手段が起動されないため、必要以上にメモリ容量を消費せず、そのために実行速度が低下するなどの弊害が生じない。

- [0081] 上記システムは、生体として動物を用いた薬品の毒性試験に好適に用いられる。上記毒性試験は、膨大で多種多様なデータが存在し、ユーザによって必要なデータの種類が異なることが多いが、このシステムによれば、使用する可能性の高い必要なプログラムだけ導入でき、システム全体のコストを大幅に引き下げることができるからである。また、複数の観察者が交代でデータ入力等を行うことが多いため、一定期間ごとに入力者等が確認できる本発明の効果が顕著であり、効果的だからである。
- [0082] 図5は、上記システムにおいて自動検査すなわちオートバリデーションを行うときのフローチャートである。
- [0083] ここで、バリデーションステップとしては、以下のようなものがある。
- ・設計の適格性確認 (DQ) … 要求仕様・機能仕様・性能仕様・メーカ選定基準装置の購入前・仕様目的を変更する際
 - ・導入時の適格性確認 (IQ) … 注文書との照合・ハードとソフトの据付確認時・システムをアップグレード後・システム移設後
 - ・稼動性能適格性確認 (OQ) … 重要機能ルーチン使用する前・最低年に1度
 - ・稼動時適格性確認 (PQ) … 使用目的毎の性能・予防保守・使用時の稼動性能確認ルーチンの前と稼動中・毎日又は、使用時
- [0084] すなわち、バリデーションは、導入時の適格性確認 (IQ) だけでなく、運用中の適格性確認 (OQ・PQ) が、重要となってくる。たとえば、システムが表計算ソフトと連携している場合、表計算ソフトのバージョンが代わった場合も適格性確認をしなければならない。場合によっては、連携していないにもかかわらず、WWWブラウザソフトをアップデートしたら確認する必要がある。このように、変化した際に、バリデーションをする方式では、ユーザが知らない間に変更があった場合に、対応することが出来ない。そこで、TOXランチャーでは、定期的にバリデーションを自動で行えるようにしている。具体的には、バリデーションの手順を記録やプログラミングし、その結果判定までする機能を付加する。
- [0085] まず、マウスやキーボード等からの検査実行信号の入力 (もしくは前記ランチャープログラムからの周期的な自動起動命令) により、各検査シナリオ28が検査シナリオ格納部17から読み出される (S1)。そして、読み出された複数の検査シナリオのうち、最

初の単位検査シナリオa(図3参照)の実行が開始される(S2)。つぎに、実行された検査シナリオにおいて、当該検査シナリオaが検査対象とするアプリケーションAに対して擬似信号を入力し、上記アプリケーションAによる擬似信号に対する応答信号を検知する(S3)。

[0086] つぎに、検知した応答信号を検査結果格納部20に格納された検査結果と対比してシステム運用中の変化の有無を判定する。このとき、上記応答信号が、最初の受入検査時に設定した基準範囲内であるかの判定が行われ(S4)、基準範囲内であれば、システムの運用に影響しない変化として変化とみなさず無視し、ステップ6に進んで検査を実行する。一方、上記応答信号が、上記基準範囲を越えたものであれば、システムの運用に影響する変化としてNG出力を行った後(S5)、ステップ6に進んで検査を実行する。上記NG出力は、例えば、ディスプレイ等の表示手段4に、該当するアプリケーション名、該当箇所、変化の内容等を特定して表示し、それに対するユーザの確認の事実をプリンタ等の出力手段3によって出力し、またはログとして記録することにより行われる。

[0087] なお、NG出力に基づく表示を行った後に、所定時間が経過してしまい、前記認証手段10が再度の認証をユーザに要求することがある。この場合、異なるユーザがログインすることも可能であり、その場合にはこの異なるユーザ名が前記NG及びその確認の事実に関連付けられて記録される。これにより、誰が確認を行ったかの事実を正確に記録することができる。したがって、ユーザを厳しく管理したい場合には、前記認証手段10による認証確認の間隔を短く設定することが好ましい。

[0088] そして、1つの単位プログラムaが終了すると(S7)、今回の動作確認結果および対比結果を出力手段3で出力するとともに、検査結果格納部20に格納し保存することが行われるとともに、すべての単位プログラム(図3の例ではa, b, c)がすべて終了したか否かを判断し(S8)、すべてが終了していなければステップ2に戻って次の単位プログラムbの実行を開始し、すべてが終了していれば自動検査を終了する。

[0089] このように、上記安全性試験支援システムによれば、2回目以降の動作確認を自動的に行うことにより、従来2〜3名の人員で3ヶ月以上の時間を要していたものが、1晩足らずで終了するようになる。したがって、システム運用中の定期的な動作確認だけ

でなく、オペレーションシステムや連携していない他のソフトウェアをアップデートした際にも、頻繁に動作確認を行い、確実にGLP等を保証することができるようになる。また、こまめに動作確認できるため、汎用機を使用できるようになり、システムの導入コストを大幅に引き下げることができる。

- [0090] また、受け入れ検査時に必然的に行われる動作確認の手順を記憶して2回目以降の動作確認を行うため、画一的なパッケージシステムではなく、システム受け入れ先ごとにカスタマイズされたシステムであっても、各受け入れ先ごとに必要な動作確認を2回目以降自動的に行うことができる。
- [0091] このような安全性試験支援システムは、生体として動物を用いた薬品の毒性試験に好適に用いられる。生体として動物を用いた薬品の毒性試験が、膨大で多種多様なデータ処理が必要であることから、システムの導入コストが低いことが求められ、汎用機を使用できる効果が顕著で効果的だからである。
- [0092] なお、本発明のシステムは、生体として動物を用いた薬品の毒性試験だけに限らず、動物による安全性試験に入る前の薬効薬理試験や一般薬理試験、薬物動態試験、あるいは、GCP(医薬品の臨床試験の実施に関する基準)が適用される臨床試験等にも応用することができる。また、非GLPの試験に応用することも可能である。これらの場合でも、同様の作用効果を奏する。
- [0093] また、本発明において、薬品とは、医薬品に限定されるものではなく、農薬、食品添加物、皮膚外用剤をはじめ、各種の化学物質を含む趣旨である。
- [0094] また、上記各実施の形態では、プログラムを起動する動作(ステップ10〜40)、プログラムの起動を確認する動作(ステップ90〜160)、業務プログラムを起動する動作(ステップ50〜80)等の動作を一連のルーチンで説明したが、それぞれ別個の実行形式で非同期で実行される場合も含む趣旨である。
- [0095] また、上記各実施の形態では、認証情報の入力を、キーボードを用いてパスワードを入力することにより行ったが、これに限定するものではなく、磁気カードやICカード等のIDカード、指紋・声紋・網膜等の認識装置によって行うこともできる。たとえば、マウスに指紋認証手段を組み込んでおくことにより、ユーザに対して認証画面を頻繁に表示することなく、上記の周期的な認証を実行することができる。

図面の簡単な説明

[0096] [図1]本発明の安全性試験支援システムの一実施の形態を示すシステム構成図である。

[図2]アプリケーション起動手段による表示画面の一例を示す図である。

[図3]上記安全性試験支援システムの作用を説明する図である。

[図4]上記安全性試験支援システムの動作を説明するフローチャート図である。

[図5]上記安全性試験支援システムの動作を説明するフローチャート図である。

符号の説明

- [0097]
- 1 データ入力手段
 - 2 アプリケーション実行手段
 - 3 出力手段
 - 4 表示手段
 - 5 アプリケーション格納部
 - 6 データ格納部
 - 7 アプリケーション起動手段
 - 8 アプリケーション選択手段
 - 9 起動確認手段
 - 10 使用者認証手段
 - 11 認証情報入力手段
 - 12 記憶装置
 - 13 演算部
 - 14 メニュー
 - 15 アイコン
 - 16 画面
 - 17 検査シナリオ格納部
 - 18 認証情報保持手段
 - 19 検査実行手段
 - 20 検査結果格納部

- 21 デバイス
- 22 ドライバ
- 23 オペレーションシステム
- 27 アプリケーション
- 28 検査シナリオ
- 29 プログラム導入手段

請求の範囲

- [1] コンピュータシステム上で実行される1もしくはそれ以上のアプリケーションプログラムのいずれか1つもしくはそれ以上に所定の変更がなされたか否かを検出するためのコンピュータソフトウェアプログラムであって、
- 記憶媒体と、
- 前記記憶媒体に格納され、前記アプリケーションプログラムのうち少なくとも最初の1つを実行する前にユーザの認証を行い、以後実行されるアプリケーションプログラムに前記認証にかかるユーザを関連付ける認証プログラムと、
- 前記記憶媒体に格納され、各アプリケーションプログラムに関連付けられ、各アプリケーションプログラムに所定の変更がなされたかを検出するための検査シナリオと、
- 前記記憶媒体に格納され、検査プログラムが関連付けられた所定のアプリケーションプログラムを前記検査シナリオに従って実行させることにより、そのアプリケーションプログラムに所定の変更がなされたかを検知させ、その検知結果を前記ユーザ名及びアプリケーションプログラムと関連付けて出力させる検査プログラムと、
- を有することを特徴とするコンピュータソフトウェアプログラム。
- [2] 請求項1記載のコンピュータソフトウェアプログラム製品において、
- 前記1もしくはそれ以上のアプリケーションプログラムは、他のアプリケーションプログラムをユーザに選択実行可能に表示するアプリケーションプログラムランチャーを含むものである。
- [3] 請求項1記載のコンピュータソフトウェアプログラムにおいて、
- 前記1もしくはそれ以上のアプリケーションプログラムは、同一ポリシーの下で所定の基準を満たすために動作確認が必要な複数のアプリケーションプログラムを有し、
- 前記検査シナリオは、各アプリケーションプログラムになされた変更が、このアプリケーションプログラムを再度の動作確認を行うことなく実行することを許容する程度のものか否かを検出するためのものであり、
- 前記検査プログラムは、そのアプリケーションプログラムに、前記検出シナリオに従って、動作確認を行うことなく実行することを許容する程度以上の変更がなされたと検出したときに、前記そのことを表示するように前記コンピュータシステムに指令するも

のである。

- [4] 請求項1記載のコンピュータソフトウェアプログラムにおいて、
前記検査プログラムは、前記検査シナリオに従って、前記アプリケーションプログラムに擬似信号を入力し、上記入力した擬似信号に対する応答信号を検査することにより、アプリケーションプログラムに所定の変更がなされたかを検知させるものである。
- [5] 請求項4記載のコンピュータソフトウェアプログラムにおいて、
前記検査シナリオは、検査するアプリケーションプログラムを特定するための情報と、そのアプリケーションプログラムに擬似信号として入力する情報と、そのデータに対する応答に関する許容範囲に関する情報を少なくとも含むものである。
- [6] 請求項1記載のコンピュータソフトウェアプログラムにおいて、
前記検査プログラムは、所定の周期で起動されるものである。
- [7] 請求項1記載のコンピュータソフトウェアプログラムにおいて、
前記検査プログラムは、前記検知結果をコンピュータディスプレイ上に表示させる検知結果表示部と、当該検知結果に対するユーザの入力を受け取って前記検知結果と関連付けて出力するユーザ入力出力部とを有する。
- [8] 請求項1記載のコンピュータソフトウェアプログラムにおいて、
前記認証プログラムは、
所定時間毎にユーザに認証情報の入力を求める認証更新要求部を有し、
前記認証更新要求部でユーザの認証ができない場合には、当該ユーザに関連付けられた実行中の前記アプリケーションプログラムを終了させるようになっている。
- [9] 請求項1記載のコンピュータソフトウェアプログラムにおいて、
前記認証プログラムは、
最初のユーザ認証の後に、ユーザの要求に応じて再度ユーザ認証を行い、現在実行されているアプリケーションプログラム及び以後実行されるアプリケーションプログラムに前記認証にかかるユーザを関連付けるものである。
- [10] 請求項1記載のコンピュータソフトウェアプログラムは、安全性試験の結果が前記アプリケーションプログラム中で改ざんされていないことを保証するためのものであり、
前記アプリケーションプログラムは、安全性試験用の計測デバイスから改ざんされて

いない計測値を受け取りこの測定値を処理して所定の処理結果を出力するものである。

- [11] 互いに関連する1もしくはそれ以上のアプリケーションプログラムを格納するアプリケーション格納部と、

前記アプリケーションプログラムのうち少なくとも最初の1つを実行する前にユーザの認証を行い、以後実行されるアプリケーションプログラムに前記認証にかかるユーザに関連付ける認証部と、

各アプリケーションプログラムに関連付けられ、各アプリケーションプログラムに所定の変更がなされたかを検出するための検査シナリオを格納する検査シナリオ格納部と、

検査プログラムが関連付けられた所定のアプリケーションプログラムを前記検査シナリオに従って実行させることにより、そのアプリケーションプログラムに所定の変更がなされたかを検知させ、その検知結果を前記ユーザ名及びアプリケーションプログラムと関連付けて出力させる検査部と、

を有することを特徴とするアプリケーションプログラム検査システム。

- [12] 互いに関連し、コンピュータシステム上で実行される1もしくはそれ以上のアプリケーションプログラムのいずれか1つもしくはそれ以上に所定の変更がなされたか否かを検出するための方法であって、

前記アプリケーションプログラムのうち少なくとも最初の1つを実行する前にユーザの認証を行い、以後実行されるアプリケーションプログラムに前記認証にかかるユーザに関連付ける認証工程と、

各アプリケーションプログラムに関連付けられ各アプリケーションプログラムに所定の変更がなされたかを検出するための検査シナリオを用い、検査プログラムが関連付けられた所定のアプリケーションプログラムを前記検査シナリオに従って実行させることにより、そのアプリケーションプログラムに所定の変更がなされたかを検知させ、その検知結果を前記ユーザ名及びアプリケーションプログラムと関連付けて出力させる検査工程と、

を有することを特徴とする方法。

[図2]

● Tox Lunch

臨床症状観察

病理

体重

臓器重量

ツール

計画

安全性試験

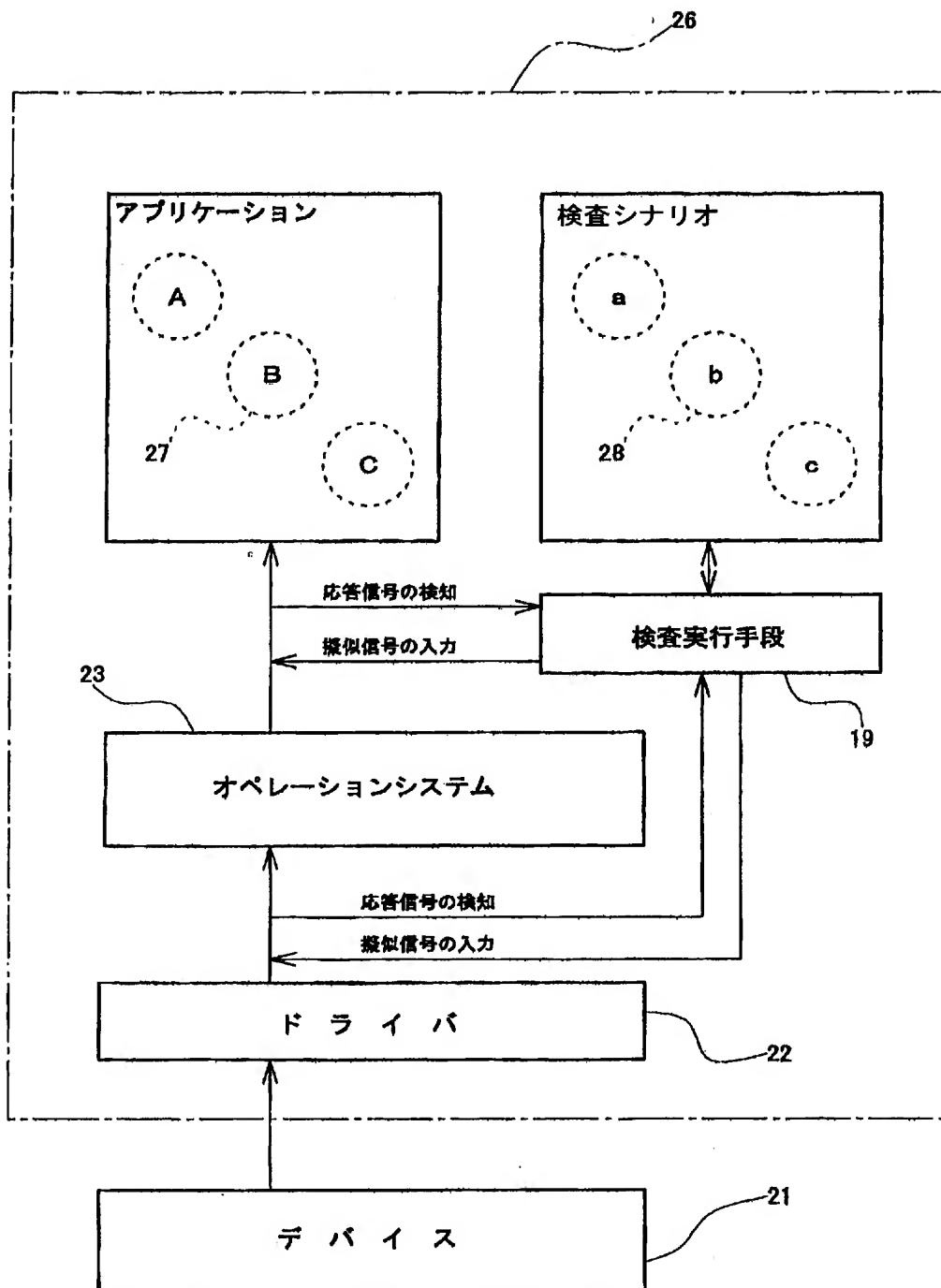
	基本データ入力				
	臨床症状観察 所見入力				
	臨床症状観察 日報・個別印刷				
	臨床症状観察 日常・個別更新				
	臨床症状観察 日報・通常印刷				
	臨床症状観察 基本所見マスク				
	帳票作成				
			臓器重量	今回測定動物	

16

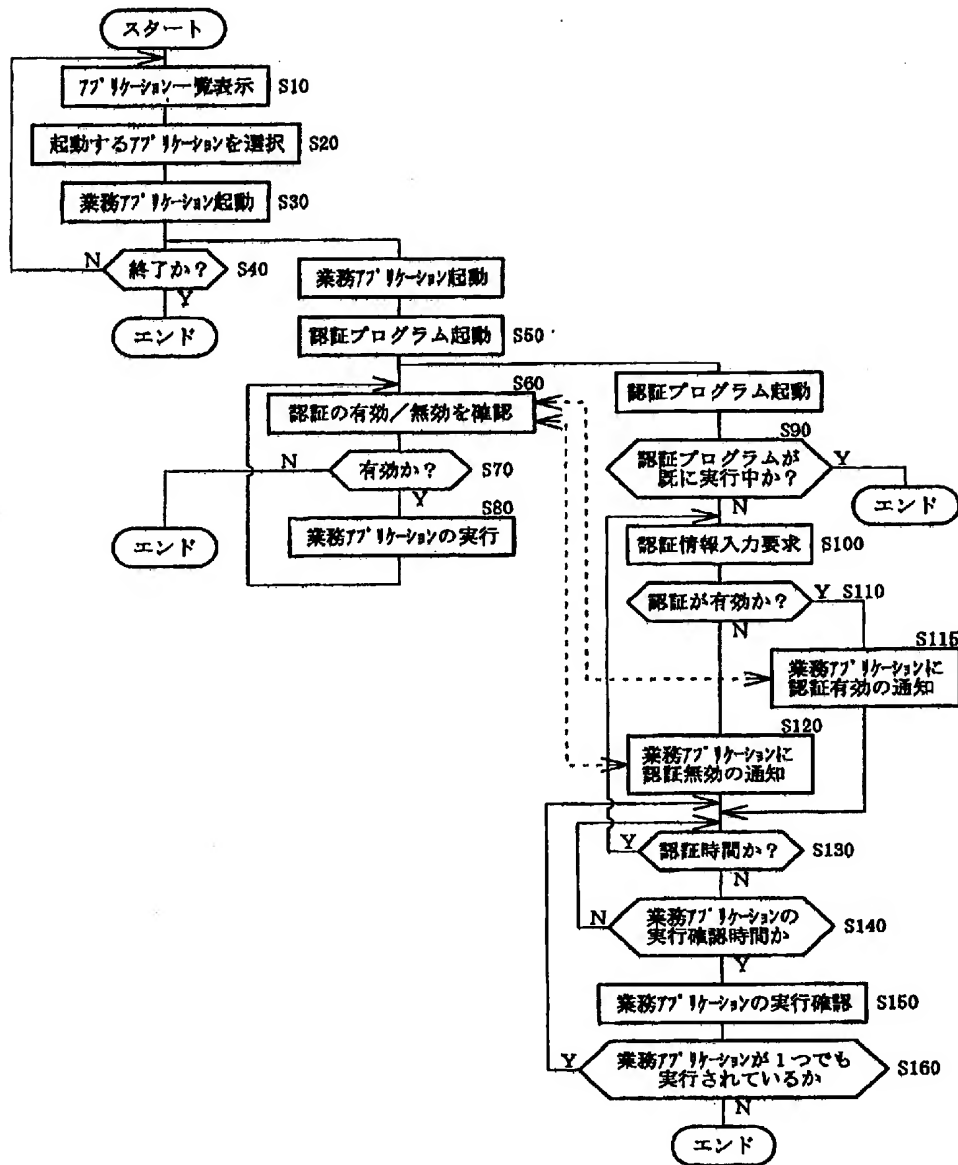
14

15

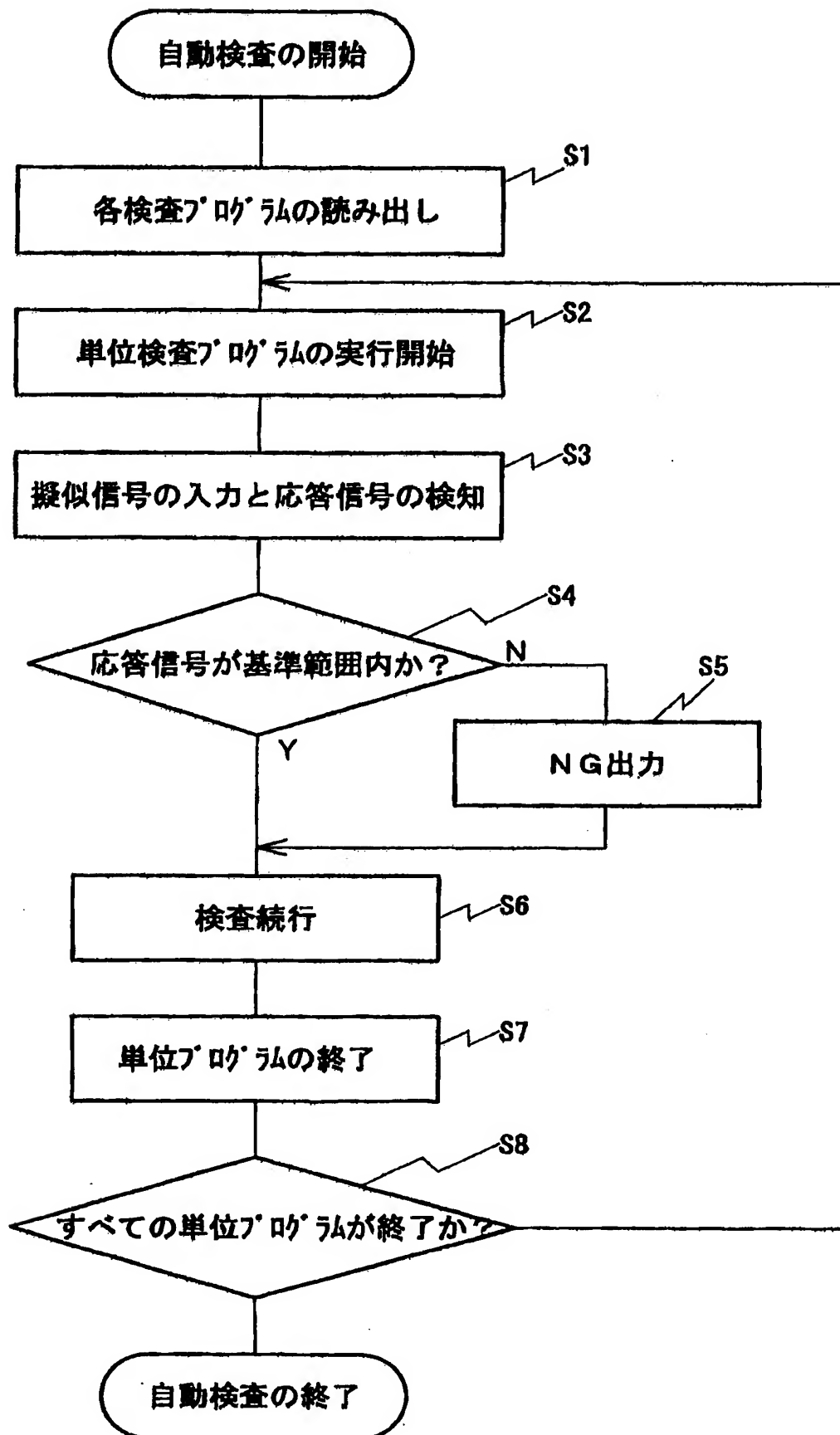
[図3]



[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/019565

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F11/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F11/30, G06F11/28, G06F17/60, G01N33/15

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Kiyoshi MURAKAMI, Haruo SUZUKI, Yoshiaki UENO, Ryoichi HAGA, "Tokushu Iyaku hin Seizogyo ni Okeru Keisoku-Seigyo-Joho System:Iyaku hin Keisoku Seigyo System to Senjo Variation", Hitachi Hyoron, 01 April, 1996 (01.04.96), Vol.78, No.4, pages 71 to 76, ISSN 0367-5874 (Tokuni Dai 4 Sho o Sansho)	1-12
Y	JP 2001-350650 A (NTT Comware Corp.), 21 December, 2001 (21.12.01), Par. No. [0017]; Fig. 12 (Family: none)	1-12

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier application or patent but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
28 February, 2005 (28.02.05)

Date of mailing of the international search report
15 March, 2005 (15.03.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/019565

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-188680 A (Kabushiki Kaisha H & T et al.), 10 July, 2001 (10.07.01), Par. Nos. [0020] to [0041] (Family: none)	2-6, 8-10
Y	JP 2001-116744 A (Kabushiki Kaisha H & T et al.), 27 April, 2001 (27.04.01), Par. Nos. [0002] to [0031] (Family: none)	4-6, 10
Y	JP 5-94298 A (NEC Hokuriku Software Co., Ltd.), 16 April, 1993 (16.04.93), Fig. 3; Par. No. [0008] (Family: none)	4, 5
Y	JP 7-13809 A (NEC Corp.), 17 January, 1995 (17.01.95), Par. No. [0036] (Family: none)	5
Y	JP 2000-275253 A (Kabushiki Kaisha Horiba Seisakusho), 06 October, 2000 (06.10.00), Par. Nos. [0023], [0026], [0031] (Family: none)	7

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int.Cl. ⁷ G06F11/30		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int.Cl. ⁷ G06F11/30、G06F11/28、G06F17/60、G01N33/15		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2005年 日本国実用新案登録公報 1996-2005年 日本国登録実用新案公報 1994-2005年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	村上 聖、鈴木春生、上野良明、芳賀良一、特集 医薬品製造業における計測・制御・情報システム：医薬品計測制御システムと洗浄バリデーション、日立評論、1996.04.01, Vol.78, No.4, pp.71~76, ISSN 0367-5874 (特に第4章を参照)	1-12
Y	JP 2001-350650 A(エヌ・ティ・ティ・コムウェア株式会社) 2001.12.21, 第17段落及び第12図 (ファミリーなし)	1-12
Y	JP 2001-188680 A(株式会社エイチ・アンド・ティー 外1名) 2001.07.10, 第20~41段落 (ファミリーなし)	2-6, 8-10
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	国際調査報告の発送日	
28.02.2005	15.3.2005	
国際調査機関の名称及びあて先	特許庁審査官 (権限のある職員)	5 B 9 2 8 8
日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	坂庭 剛史	
	電話番号 03-3581-1101	内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-116744 A(株式会社エイチ・アンド・ティー 外1名) 2001. 04. 27, 第2～31段落 (ファミリーなし)	4-6, 10
Y	JP 5-94298 A(北陸日本電気ソフトウェア株式会社) 1993. 04. 16, 第3図及び第8段落 (ファミリーなし)	4, 5
Y	JP 7-13809 A(日本電気株式会社) 1995. 01. 17, 第36段落 (ファミリーなし)	5
Y	JP 2000-275253 A(株式会社堀場製作所) 2000. 10. 06, 第23, 26, 31段落 (ファミリーなし)	7